

**ARC 605P**

Digital Student Data Transfer Procedure

**PURPOSE**

Establishes the procedure for transferring student data-sets that include more than a few students, both internally and externally, at Clackamas Community College following privacy and security best practices.

**PROCEDURE**

When a CCC employee needs to send more than a few student records electronically they should refer to the data transfer protocol for specifics: [Data-Transfer-Protocol-for-ARC-605P](https://intranet.clackamas.edu/docs/librariesprovider2/registrar's-office/data-transfer-protocol-for-arc-605p.pdf?sfvrsn=2e6b9d68_1) or contact the Registrar at [registrar@clackamas.edu](mailto:registrar@clackamas.edu) for assistance.

Unencrypted methods of data transfer, such as email, should not be used for transferring student datasets.

Student datasets should not be stored on thumb drives or other external hard drives.

FERPA information includes Student ID, Social Security Number (SSN), transcripts, financial aid records, etc. Generally, information that contains FERPA information should not be sent by email.

If an electronic data breach is suspected or occurs, the employee should immediately notify the CCC Registrar at [registrar@clackamas.edu](mailto:registrar@clackamas.edu).

**DEFINITIONS**

“A few students” are defined as 5 or less and would have the lowest amount of impact and harm in the case of a data breach. Allowing the use of email for a few students will reduce the impact on day-to-day processes.

“Student data” is defined as anything related to the student, including contact, demographic, and all academic information.

**Applicability**

This policy applies to all College employees.

**Enforcement**

In the event of a data breach, the appropriate CCC employee will work with the Registrar and appropriate authorities to take the following actions:

* Determine what information was compromised.
* Take immediate steps to retrieve data and prevent further disclosures.
* Identify which policies and procedures may have been breached.
* Identify all affected records and students.
* Report to legal authority.
* Connect with responsible parties and clarify oversight and accountability.
* Risk assessment of further breaches.
* Notify students of the breach and remediation options.
* The Registrar is required to make a note on the student record.

**RELATED**

Current CCC [FERPA policy](https://www.clackamas.edu/docs/default-source/about-us/accreditation-and-policies/ccc-ferpa-policy.pdf?sfvrsn=919479b9_0) and CCC Board of Education policy on [directory information](https://policy.osba.org/clackcc/J/JOA%20G1.PDF)

**END OF PROCEDURE**

**APPROVALS**

|  |  |
| --- | --- |
| Maintained By | Access, Retention, and Completion Committee (ARC) |
| ARC Initial Review | November, 2023 |
| ISP Committee – if appropriate |  |
| College Council – first reading |  |
| College Council – second reading |  |
| President’s Council – if appropriate |  |
| Final ARC Review and Approval |  |